学校编码：10384
学号：23120111153023

分类号___密级_____
UDC_____

厦门大学

硕 士 学 位 论 文

# AES 算法的硬件优化实现及应用研究

# Research on Hardware Optimization Implementation and Application of AES Algorithm

郑行

指导教师姓名：王云峰 副教授
专 业 名 称：电 路 与 系 统
论文提交日期：2014 年 5 月
论文答辩时间：2014 年 5 月
学位授予日期：2014 年 6 月

答辩委员会主席：
评 阅 人：

2014 年 5 月

# 厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：郭行

2014 年 5 月 26 日

# 厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：郑行

2014 年 5 月 26 日

# 摘 要

随着计算技术与网络的高速发展，计算机和通信网络的应用不仅仅局限于银行、航空、政府、军事等重要部门，而是进入了人们的日常生活的方方面面。网络信息交换已成为人们获取和交换信息的主要形式，信息安全也越来越得到人们的重视。在解决信息安全问题中，密码技术提供关键理论与技术，在信息安全领域有着不可替代的作用。高级加密标准 AES 作为一种密码技术，具有抗攻击能力强、易于硬件实现、加密速度快、可移植性强等优点，受到了国内外的广泛研究。因此，高性能的 AES 实现及其应用已经成为当前信息安全的研究热点。

为了防止国外 AES 硬件产品中可能存在的“陷门”，开展 AES 硬件实现的自主研究很有必要。针对网络应用的需要，如何实现高性能 AES 及其应用为本文的研究重点。具体工作内容如下：

1、为了降低面积复杂度，减少资源占用，采用复合域组合逻辑来实现非线性的字节代换和逆字节代换；采用复用技术来实现 AES 中字节代换和逆字节代换、列混合和逆列混合。

2、进行了轮单元的 7 级流水划分。在此基础上，完成了完全环展开与反馈模式下的循环迭代两种 AES 硬件实现方案。完全环展开方案具有较高的工作频率；循环迭代方案的吞吐率面积比比较大。

3、在密钥扩展方面，为了不降低 AES 的吞吐率，采用复合域算法和 7 级流水线设计，可实时为 AES 提供加密轮密钥。

4、基于消息认证，进行了可用于电子商务交易系统的安全协议研究。并完成了支持协议的终端硬件设计，可实现高速数据认证、加密/解密、数字签名与完整性检测。

**关键词：**AES；流水线；复合域算法；信息安全；认证协议

# ABTRACT

With the fast development of computing technology and network, computers and communication network are used more and more widely in normal life. Online information interchange has become the main access for people to acquire information, and importance of information security has been revalued. Cryptology, which offers the key theory and technology, is irreplaceable in information security. AES is easy to be implemented in hardware and transplanted. Moreover it has a good anti-attacking capability and a high encryption speed. So AES is widely researched and high-performance AES has become the research focus in information security.

To avoid the risk caused by probable dropdoor of abroad AES products, independent intellectual property in AES is very necessary. So this paper focuses on design of high-performance AES implementation for network application. The concrete content is as follow:

Combinatorial logic of composite field and reuse technology are used in SubBytes and InvSubBytes to reduce the area and resources; reuse technology is used in MixColumns and InvMixColumns.

Round unit is divided into seven stages pipelining, and AES hardware implementations of full loop-unrolling and loop iteration of feedback mode are made; the scheme of full loop-unrolling has a relatively high working frequency while the scheme of loop iteration has a better throughout area ratio.

In key expansion, composite field algorithm and seven stages pipelining are used to avoid the reduction in throughout and offer real-time encryption roundkeys.

Based on message authentication, researches on security protocol for electronic commerce transaction system and hardware design of corresponding terminals are made. The design is able to realize high-speed data authentication, encryption and decryption, digital signature and integrity detection.

**Keywords**: AES; Pipelining; Composite Field Algorithm; Information Security; Authentication Protocol

# 目录

# CONTENTS

# 第一章　绪论

## 1.1　研究背景及其意义

随着信息全球化，计算机网络技术的日益普及，其应用范围包括社会的诸多领域，如金融业务系统、政府部门系统和企业部门系统等等[1]。在当今的信息化时代，信息安全问题不但关系到一国政治、经济、社会乃至国防等方面的安全，而且随着个人电子交易在网络中日益频繁，保障个人在网络中的安全也变得愈加重要。因此，谁掌握了信息安全，谁就在信息时代占据了制高点，从而拥有“制信息权”[2]。随着网络应用的不断深入，网络信息安全逐渐受到人们的重视，而网络自身的自由性与开放性等特点，使得提高用户安全交易的难度大为增加[3]。

在信息安全中，密码学起着核心的作用[4]，可以提供安全协议设计必须的四种基本安全服务，即数据机密性、消息完整性、身份认证、不可否认性。数据机密性可以通过对敏感消息加密的方式生成秘密消息，即使秘密消息被截获也不能得到消息的内容；消息完整性就像生活中的报警器一样，检测消息是否被修改，这功能可由散列函数进行实现；身份认证如飞机登机牌领取时出示身份证一样，应用密码学的身份认证技术可以实现这一服务；不可否认性是数字签名[5]实现，可以防止抵赖，它像现实签到协议文件的签字一样，可作为违约的证据。

密码学加密技术就密钥的策略上而言，密码体制可分为对称密码体制和非对称密码体制[6]。其中对称密码体制中高级加密标准[7]（AES）在信息安全中起着重要的作用，有着以下优点[4]：

（1）加密和解密速度快，有很高的数据吞吐率，便于软硬件实现；

（2）密文和明文长度相同；

（3）其算法安全性能在现有的攻击下能保持良好的安全性。

AES 的这些优点，既可以满足网络对数据安全性的要求，又可以满足网络高速数据处理速度的要求。因此，AES 算法除了作为加密信息之外，还可以作为信息与网络安全中消息认证、数字签名及密钥管理的核心密码算法，它在计算机通信和信息系统安全领域有着广泛的应用[8]。

当前电子商务交易系统中存在的安全问题，是阻碍电子商务发展的主要问题

[9]。由于网络的开放性，电子商务必须着重考虑传输数据的安全，以达到安全交易的目的。以网络交易为例，交易信息或银行卡信息泄漏等安全问题是很多用户深感担忧的首要问题。除此以外，如何在电子交易前确认对方身份，并在交易产生后进行消息完整性认证和交易双方不可否认性确认等问题，都威胁着交易安全，是需要考虑与解决的问题。

为了使电子交易能够安全进行，需要满足以下条件。第一，所有电子商务参与者之间（包括用户和服务方），首先进行身份认证，待确认身份无误后，才能进行相应的数据访问和管理[10]。第二，保证相互交易的双方信息保密。第三，必须保证电子商务交易记录的长期完整性，以防欺诈行为，从而提高电子交易的可信度[11]。AES 算法具有良好的硬件实现特性，它有效地满足电子商务在安全和速度方面的要求。一方面，AES 可以加密数据信息，实现信息的保密性；另一方面，AES 的高速数据处理速度可以满足电子商务实时和高速的需要[12]。以 FPGA 的实现方案具有灵活性和易维护性优点，因此可以将 FPGA 作为研究和实现 AES 算法理想的硬件平台[13]。

信息安全是个特殊的领域，无论是在密码算法上还是在其硬件实现上，都有可能存在“陷门”即“后门”[14]，从而造成安全隐患。所谓“陷门”是一个模块实现的秘密入口，其目的是为了测试或者增强这个模块，从而给设计者未来修改或升级设计提供方便。陷门的设定，使得提供特定的输入数据时，允许违反安全策略[15]。通常在开发设计完成时应去掉陷门，但由于某些考虑及原因，陷门可能被保留下来，一旦被恶意利用势必给用户的信息安全造成严重的后果[16]。因此，开展自主设计高性能密码算法硬件实现显得非常必要。出于以上考虑，国内外研究机构纷纷加强对密码学算法的研究，其目的在于完全自主设计密码算法的硬件实现。因此，本文设计的高性能 AES 硬件实现及应用研究具有一定的实际意义。

## 1.2 AES 发展及研究现状

1997 年，美国政府开始公开征集新的数据加密标准算法 AES[7]，其目的在于取代不能满足安全服务的 DES[17]。2000 年 10 月 2 日，美国政府正式宣布选择比利时密码学家 Joan Daemen 和 Vincent Rijmen 共同发明的 Rijndael 算法作为新